

ON TORSION-FREE NILPOTENT LOOPS

JACOB MOSTOVOY, JOSÉ M. PÉREZ-IZQUIERDO, AND IVAN P. SHESTAKOV

ABSTRACT. We show that a torsion-free nilpotent loop (that is, a loop nilpotent with respect to the dimension filtration) has a torsion-free nilpotent left multiplication group of, at most, the same class. We also prove that a free loop is residually torsion-free nilpotent and that the same holds for any free commutative loop. Although this last result is much stronger than the usual residual nilpotency of the free loop proved by Higman, it is proved, essentially, by the same method.

1. INTRODUCTION

It has been argued [7] that the usual definition of nilpotency in loops, given by Bruck [2] is too weak for the most important properties of nilpotent groups to hold. Indeed, contrary to what happens in the associative case, the successive quotients of Bruck's lower central series of a general finitely generated loop are not finitely generated; moreover, they do not carry any algebraic structure similar to that of a Lie ring.

A different version of the lower central series, designed to eliminate these drawbacks, was introduced in [7] under the name of the *commutator-associator filtration* (in much greater generality, this definition was later independently stated by Hartl and Loiseau [4]). An important feature of this filtration is its close relationship with the *dimension filtration* which is defined via the powers of the augmentation ideal in the loop ring. By a theorem of Jennings, If G is a group, the dimension filtration of G collapses after n th term if and only if G is torsion-free nilpotent of class n ; the same holds for loops if by nilpotency one understands the nilpotency with respect to the commutator-associator filtration [8]. It is therefore reasonable to call a loop *torsion-free nilpotent of class n* if its dimension filtration collapses after the n th term.

In the present paper we prove two statements that show the usefulness of this notion. Firstly, we show that a torsion-free nilpotent loop of class n has a torsion-free nilpotent left multiplication group of class *at most* n . This fails to hold for torsion-free nilpotent loops in the sense of Bruck, a counterexample being the free nilpotent (in the sense of Bruck) loop of class two, whose left multiplication group is not nilpotent. We stress that the nilpotency class of the left multiplication group may be strictly less than the class of the loop; examples of such situation will be given.

Our second (and most important) result says that a free loop is residually torsion-free nilpotent (and, in particular, residually nilpotent with respect to the commutator-associator

2010 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Loops, nilpotent loops, torsion-free nilpotent loops.

The authors acknowledge the support by the Spanish Ministerio de Ciencia e Innovación (MTM2013-45588-C3-3-P); J. M. Pérez-Izquierdo also thanks support by PHBP14/00110; J. Mostovoy was also supported by the CONACYT grant 168093-F; I. P. Shestakov also acknowledges support by FAPESP, processo 2014/09310-5 and CNPq, processos 303916/2014-1 and 456698/2014-0.

filtration). This statement is much stronger than the assertion that free loops are residually nilpotent in the sense of Bruck, proved by Higman in [5], although our proof is an application of the same arguments (Higman was well aware that his methods were stronger than what was necessary for the study of Bruck's lower central series). A similar result is then proved for free commutative loops.

Our main technical tool is the non-associative modification of the Magnus map from the free group on k letters to the group of units in the ring of non-commutative power series in k variables. We will use some very basic facts about loops and about non-associative Hopf algebras as described in [11], although we shall give some definitions in order to fix the notation.

2. PRELIMINARIES

2.1. Torsion-free nilpotent loops. A *loop* L is a set with a unital, not necessarily associative, product, such that both left and right multiplications

$$L_a: L \rightarrow L, \quad x \mapsto ax$$

$$R_a: L \rightarrow L, \quad x \mapsto xa$$

by any $a \in L$ are bijective. In a loop one defines the operations of left and the right division by setting

$$a \backslash x = L_a^{-1}x$$

and

$$x/a = R_a^{-1}x$$

respectively. With each loop L one associates its *left multiplication group* $\text{LMlt}(L)$: this is the subgroup of the permutation group of L considered as a set, which is generated by the L_a for all $a \in L$.

Extending the loop product in a loop L by linearity to the \mathbb{Q} -vector space spanned by L , one obtains the loop algebra $\mathbb{Q}L$. In the loop algebra, the *augmentation ideal* I is the kernel of the homomorphism $\mathbb{Q}L \rightarrow \mathbb{Q}$ which sends each element of L to 1. The n th power I^n of the augmentation ideal is the ideal spanned by the products of at least n elements of I . The *n th dimension subloop of L over \mathbb{Q}* is defined as

$$D_n L = \{g \in L \mid g - 1 \in I^n\}.$$

We shall refer to these subloops simply as to dimension subloops, without any mention of the field \mathbb{Q} . For each n the subloop $D_n L$ is normal (and fully invariant) in L and each quotient $D_n L / D_{n+1} L$ is torsion-free [9]. The loop L is called *torsion-free nilpotent of class n* if $D_{n+1} L$ is trivial while $D_n L$ is not.

2.2. Free loops and the Magnus map. Let $\mathbf{x} = \{x_1, \dots, x_n\}$. The set $W(\mathbf{x})$ of *words* on \mathbf{x} is defined recursively so as to consist of (a) all elements of \mathbf{x} and e ; (b) all expressions of the form uv , $u \backslash v$ and u/v where u and v belong to $W(\mathbf{x})$. The set $W(\mathbf{x})$ is the free algebra on \mathbf{x} with one nullary operation e and three binary operations. The set $\text{Comp}(w)$ of *components* of a word $w \in W(\mathbf{x})$ is defined by setting

$$\text{Comp}(e) = \{e\},$$

$$\text{Comp}(x_i) = \{e, x_i\} \text{ when } x_i \in \mathbf{x}$$

and

$$\text{Comp}(w) = \text{Comp}(u) \cup \text{Comp}(v) \cup \{w\} \text{ if } w = uv, u \setminus v \text{ or } u/v.$$

A word in $W(\mathbf{x})$ is *reduced* if none of its components is of the form

$$u \setminus (uv), u(u \setminus v), (uv)/v, (u/v)v, u/(v \setminus u), (u/v) \setminus u, ev, e \setminus v, u/e, ue, u/u, \text{ or } v \setminus v.$$

The free loop $\mathcal{F}(\mathbf{x})$ is the quotient of the algebra $W(\mathbf{x})$ by the relations

$$eu = u = ue, u \setminus (uv) = v = u(u \setminus v) \text{ and } (uv)/v = u = (u/v)v.$$

Each element of $\mathcal{F}(\mathbf{x})$ can be represented by a unique reduced word so that $W(\mathbf{x}) \subset \mathcal{F}(\mathbf{x})$; this is a corollary of the Evans Normal Form Theorem [3].

Now, let $\mathbf{X} = \{X_1, \dots, X_n\}$. Denote by $\mathbb{Q}\{\mathbf{X}\}$ the free non-associative algebra on \mathbf{X} over \mathbb{Q} and let $\overline{\mathbb{Q}\{\mathbf{X}\}}$ be its completion with respect to the degree; elements of $\overline{\mathbb{Q}\{\mathbf{X}\}}$ are non-associative formal power series in the X_i . The power series with non-zero constant term form a loop $\overline{\mathbb{Q}\{\mathbf{X}\}}^\times$ under multiplication. Explicitly, the operation of the left division in this loop is determined by

$$(1 + B) \setminus (1 + A) = 1 + (A - B) - B(A - B) + B(B(A - B)) - \dots$$

for any power series A and B with no constant term. Notice that in the case when A consists only of terms with right-normed parentheses and $B = X_i$ is one of the generators, $(1 + B) \setminus (1 + A)$ also contains terms with right-normed parentheses only.

The *Magnus map* is the homomorphism

$$\begin{aligned} \mathcal{M}: \mathcal{F}(\mathbf{x}) &\rightarrow \overline{\mathbb{Q}\{\mathbf{X}\}}^\times, \\ x_i &\mapsto 1 + X_i. \end{aligned}$$

Extending the Magnus map by linearity to any $r \in \mathbb{Q}\mathcal{F}(\mathbf{x})$ we see that $\mathcal{M}(r)$ has a zero constant term if and only if r lies in the augmentation ideal of $\mathbb{Q}\mathcal{F}(\mathbf{x})$. This implies the following:

Lemma 1 ([9]). *An element $w \in \mathcal{F}(\mathbf{x})$ lies in $D_n\mathcal{F}(\mathbf{x})$ if and only if*

$$\mathcal{M}(w) = 1 + \text{terms of degree } n \text{ and higher.}$$

In particular, in order to prove that $\mathcal{F}(\mathbf{x})$ is residually torsion-free nilpotent, it is sufficient to show that the Magnus map is injective. This is totally analogous to the associative case where the Magnus map is used to prove that the free group is residually torsion-free nilpotent [6]. However, while in the associative case this is established by a straightforward argument involving the syllable length of w , the non-associative version is somewhat more complex.

The Magnus map can be defined, in an entirely analogous fashion, for free commutative loops. Here the algebra $\overline{\mathbb{Q}\{\mathbf{X}\}}$ should be replaced by the free commutative non-associative algebra on \mathbf{X} . We shall prove that the commutative Magnus map is also injective, and this will imply that free commutative loops are residually torsion-free nilpotent.

3. THE LEFT MULTIPLICATION GROUP

Theorem 2. *If L is a torsion-free nilpotent loop of class n , the group $\text{LMlt}(L)$ is nilpotent of class at most n .*

We shall see that there are examples where the class of $\text{LMlt}(L)$ is strictly smaller than the class of L . On the other hand, when L is a group, we have $\text{LMlt}(L) = L$ and, hence, the class of $\text{LMlt}(L)$ is the same as the class of L .

The key to the proof of Theorem 2 is the following:

Lemma 3. *For all $a \in L$ and $F \in \gamma_n \text{LMlt}(L)$ we have $F(a) \equiv a \pmod{D_n L}$.*

Proof. First, let us consider the case when L is the free loop generated by a, x_1, \dots, x_n , and F is the n -fold commutator $[L_{x_1}, [\dots, [L_{x_{n-1}}, L_{x_n}] \dots]]$. Then $\mathcal{M}(F(a))$ contains right-normed terms only. By dropping the parentheses we get the associative Magnus map of the element

$$[x_1, [\dots, [x_{n-1}, x_n] \dots]] \cdot a$$

in the free group generated by a, x_1, \dots, x_n ; this series is of the form

$$1 + a + \text{terms of degree } n \text{ and greater.}$$

This implies that $\mathcal{M}(F(a))$ is also of the same form. Indeed, the homomorphism of the free non-associative algebra on a certain set of generators onto the free associative algebra on the same generators which “forgets the parentheses” maps the space of the right-normed monomials isomorphically onto the free associative algebra. This proves the lemma in this case. The exact same argument works in the case when L is the free loop generated by a, x_1, \dots, x_m , with $m \geq n$, and F is a product of arbitrary n -fold commutators in the L_{x_i} .

Now, each element $F(a)$ with $F \in \gamma_n \text{LMlt}(L)$ in an arbitrary loop L is a homomorphic image of $\tilde{F}(a)$ where \tilde{F} is a product of arbitrary n -fold commutators in the L_{x_i} in the free loop generated by a, x_1, \dots, x_m , for some m . Since the dimension subloops are respected by loop homomorphisms, the lemma follows. \square

Theorem 2 is now an easy consequence of Lemma 3. Indeed, if L is torsion-free nilpotent of class n , we have $D_{n+1}L = \{1\}$. Then, by Lemma 3, for $F \in \gamma_{n+1} \text{LMlt}(L)$ and any $a \in L$ we have $F(a) = a$, which means that F is the identity in $\text{LMlt}(L)$. Now, let us consider several examples.

Proposition 4. *Let L be the commutative loop whose elements are pairs of integers (p, q) with*

$$(p, q) \cdot (p', q') = \left(p + p', q + q' + \binom{p}{2} \binom{p'}{2} \right).$$

Then L is torsion-free nilpotent of class 4, with

$$D_2 L = D_3 L = D_4 L = \{(0, q) \mid q \in \mathbb{Z}\},$$

while $\text{LMlt}(L)$ is nilpotent of class 3.

Proof. From what follows it should become clear that L is the reduction of the free commutative loop on one generator modulo D_5 and the argument is based on the Magnus map.

Let $L_2 = \{(0, q) \mid q \in \mathbb{Z}\} \subset L$. It is clear that L_2 is a normal subloop of L (in fact, it is the centre of L) and the quotient L/L_2 is abelian and torsion-free. It follows that $D_i L \subset L_2$ for $i > 1$.

It can be seen directly that $(0, 1) \in D_4 L$. Indeed, if $X = (1, 0) - 1 \in I$, we have

$$(0, 1) - 1 = (4, 0) \setminus ((4, 1) - (4, 0)) = (4, 0) \setminus (X^2 X^2 - X^3 X),$$

which is readily seen to lie in I^4 ; see also Lemma 1 of [9]. (We can write X^3 here since, by commutativity, $X^2X = XX^2$). Since $(0, 1)$ generates L_2 , we see that $D_4L = L_2$.

Let us now show that D_5L is trivial. Let $\mathbb{Q}_c\{X\}$ be the free commutative non-associative algebra on one generator X and \mathcal{I}^k the ideal consisting of non-associative polynomials in X without terms of degree $< k$. As a vector space, $\mathbb{Q}_c\{X\}/\mathcal{I}^5$ is spanned by the monomials $1, X, X^2, X^3, X^3X$ and X^2X^2 . Consider the map

$$L \rightarrow \mathbb{Q}_c\{X\}/\mathcal{I}^5$$

given by

$$(p, q) \mapsto 1 + pX + \binom{p}{2}X^2 + \binom{p}{3}X^3 + \left(\binom{p}{4} - q\right)X^3X + qX^2X^2 \pmod{\mathcal{I}^5}.$$

A direct computation shows that it is an injective homomorphism of L into the loop of units in $\mathbb{Q}_c\{X\}/\mathcal{I}^5$. Extend it to the loop algebra $\mathbb{Q}L$ by linearity; the augmentation ideal $I \subset \mathbb{Q}L$ is then mapped to the ideal $\mathcal{I}/\mathcal{I}^5$. In particular, if $g \in D_5L$, we see that $g - 1$ maps to zero, which implies that $g = 1$.

It remains to see that $\text{LMlt}(L)$ is nilpotent of class three. On one hand, notice that $L_{(p,q)} = L_{(p,0)}L_{(0,q)}$ and that $L_{(0,q)}$ lies in the centre of $\text{LMlt}(L)$ for all q . On the other hand, we have

$$[L_{(p,0)}, L_{(r,0)}](a, b) = L_{(p,0)}^{-1}L_{(r,0)}^{-1}L_{(p,0)}L_{(r,0)}(a, b) = (a, b + \frac{1}{2}apr(p-r)).$$

Furthermore,

$$[L_{(s,0)}, [L_{(p,0)}, L_{(r,0)}]](a, b) = (a, b - \frac{1}{2}prs(p-r)).$$

It follows that $[L_{(s,0)}, [L_{(p,0)}, L_{(r,0)}]]$ lies in the center of $\text{LMlt}(L)$ and, hence, $\text{LMlt}(L)$ is three-step nilpotent. \square

Proposition 5. *Let L be the loop whose elements are pairs of integers (p, q) with*

$$(p, q) \cdot (p', q') = \left(p + p', q + q' + \binom{p}{2}p'\right).$$

Then L is torsion-free nilpotent of class 3, with

$$D_2L = D_3L = \{(0, q) \mid q \in \mathbb{Z}\},$$

while $\text{LMlt}(L)$ is nilpotent of class 2.

The proof of this proposition is very similar to that of Proposition 4, only in this example the loop in question is isomorphic to the reduction of the free *non-commutative* loop on one generator modulo D_4 ; we omit it.

Finally, we have the following fact which shows the radical difference between nilpotency in the sense of Bruck for torsion-free loops and torsion-free nilpotency for loops:

Proposition 6. *Let $L = F/F_3$ be the free nilpotent (in the sense of Bruck) loop of class 2 on a countable number of generators. Then $\text{LMlt}(L)$ is not nilpotent.*

We shall prove this assertion in the next section. Note that, by [14], for any nilpotent, in the sense of Bruck, loop L the left multiplication group $\text{LMlt}(L)$ is solvable.

4. HIGMAN'S CONSTRUCTION

Here we state several results of [5] which will be of importance.

Let $F = \mathcal{F}\{\mathbf{x}\}$ be the free loop on the set $\mathbf{x} = \{x_1, \dots, x_n\}$, $\alpha: F \rightarrow L$ a surjective homomorphism and $N = \ker \alpha$. The subloop $[N, F]$ is defined as smallest subloop of N which is normal in F and such that $N/[N, F]$ is in the centre of $F/[N, F]$. In particular, if $N = F_k$, the k th term of Bruck's lower central series, then, by definition, $[N, F] = F_{k+1}$.

Define the abelian group A to be freely generated by two types of symbols:

- x_i for each $x_i \in \mathbf{x}$;
- $\langle l_1, l_2 \rangle$ for each pair $l_1, l_2 \in L \setminus \{e\}$.

On the set $L \times A$ consider the following product:

$$(l_1, a_1)(l_2, a_2) = (l_1 l_2, a_1 + a_2 + \langle l_1, l_2 \rangle),$$

where $\langle l, e \rangle = \langle e, l \rangle = 0$ for all $l \in L$. With this product, $L \times A$ becomes a loop, which we denote by (L, A) . In particular,

$$(l_1, a_1)/(l_2, a_2) = (l_1/l_2, a_1 - a_2 - \langle l_1/l_2, l_2 \rangle),$$

$$(l_2, a_2) \backslash (l_1, a_1) = (l_2 \backslash l_1, a_1 - a_2 - \langle l_2, l_2 \backslash l_1 \rangle).$$

Consider the homomorphism

$$\begin{aligned} \delta: F &\rightarrow (L, A) \\ w &\mapsto (\alpha(w), \psi(w)) \end{aligned}$$

where $\psi(x_i) = x_i \in A$.

Lemma 7 ([5], Lemma 3).

$$\ker(\delta) = [N, F].$$

This lemma has the following corollary:

Lemma 8. $\gamma_{n-1}\text{LMlt}(F/F_3)$ is non-trivial.

Proof. Let $N = [F, F]$ so that $L = F/N$ is a free abelian group on x_1, \dots, x_n (strictly speaking, we should write $\alpha(x_i)$ instead of x_i but the notation can take some abuse) and $[N, F] = F_3$.

By Lemma 7 the image of the map $\delta: F \rightarrow (L, A)$ is isomorphic to F/F_3 . Write

$$y = [L_{x_n}, [L_{x_{n-1}}, \dots [L_{x_3}, L_{x_2}]]](x_1).$$

Then $\delta(y) = (x_1, a)$ with $a \neq x_1$. Indeed, it is easy to see (by induction on n , for instance) that the term $\langle x_2, x_1 \rangle$ appears in a with coefficient 1. This implies that the iterated commutator $[L_{x_n}, [L_{x_{n-1}}, \dots [L_{x_3}, L_{x_2}]]$ is not the identity and, hence, $\gamma_{n-1}\text{LMlt}(F/F_3) \neq \{1\}$. \square

Proposition 6 follows.

The main technical result of Higman's paper [5] is the following:

Lemma 9 ([5], Lemma 6). *Let $w, w' \in W(\mathbf{x})$ be reduced words such that*

- $w' \notin \text{Comp}(w)$,
- $\alpha(w) = \alpha(w')$,

- if u, v are words in $\text{Comp}(w) \cup \text{Comp}(w')$ such that $\alpha(u) = \alpha(v)$ then either $u = v$ or $\{u, v\} = \{w, w'\}$.

Then there exists a generator x_i or $\langle l_1, l_2 \rangle$ of A whose coefficient in $\psi(w)$ is zero, and in $\psi(w')$ is ± 1 .

This statement has a consequence which will be of immediate importance for us:

Lemma 10 ([5], Corollary 1). *Let S be a finite set of reduced words containing together with any word all of its components. If the images of the elements of S in F/N under the natural projection map are not all distinct, the number of elements in the image of S in $F/[N, F]$ is strictly greater than the number of elements in the image of S in F/N .*

5. INJECTIVITY OF THE MAGNUS MAP

Let $\mathcal{F}_c(\mathbf{x})$ be the free commutative loop on the set $\mathbf{x} = \{x_i\}$ and $\mathbb{Q}_c\{\mathbf{X}\}$ the free commutative non-associative algebra on the corresponding set $\mathbf{X} = \{X_i\}$. The commutative version of the Magnus map sends $\mathcal{F}_c(\mathbf{x})$ into the loop of invertible elements in the completion of $\mathbb{Q}_c\{\mathbf{X}\}$ and is defined exactly in the same way as the usual Magnus map: x_i is sent to $1 + X_i$.

Theorem 11. *The Magnus maps*

$$\mathcal{M}: \mathcal{F}(\mathbf{x}) \rightarrow \overline{\mathbb{Q}\{\mathbf{X}\}}^\times$$

and

$$\mathcal{M}_c: \mathcal{F}_c(\mathbf{x}) \rightarrow \overline{\mathbb{Q}_c\{\mathbf{X}\}}^\times$$

are injective.

In particular, the free loops $\mathcal{F}(\mathbf{x})$ and $\mathcal{F}_c(\mathbf{x})$ are residually torsion-free nilpotent.

5.1. Group-like elements and the modified Magnus map. Recall that in a Hopf algebra a *primitive element* is an element x satisfying

$$\Delta(x) = x \otimes 1 + 1 \otimes x$$

and a *group-like element* is an element g such that

$$\Delta(g) = g \otimes g$$

and $\epsilon(g) = 1$. The set $\mathcal{G}(H)$ of all group-like elements in a non-associative Hopf algebra H is, actually, a loop [13].

The free algebra $\mathbb{Q}\{\mathbf{X}\}$ is a Hopf algebra whose coproduct is defined by the condition that the generators are primitive. The only group-like element in $\mathbb{Q}\{\mathbf{X}\}$ is 1; however, the completion $\overline{\mathbb{Q}\{\mathbf{X}\}}$ has many group-like elements. A group-like element $e(X)$ in the algebra $\overline{\mathbb{Q}\{X\}}$ of power series in one non-associative and non-commutative variable X with a non-zero coefficient at X is called a *base for logarithms* or a *non-associative exponential series* (see [10, 12]). An example of a base for logarithms is the usual exponential series endowed with the right-normed parentheses. Given $e(X)$ there exists another series $\log_e(1 + X)$ such that $\log_e(e(X)) = X$ and $e(\log_e(1 + X)) = X$.

It will be convenient to use a slightly different version of the Magnus map by choosing a base $e(X)$ for logarithms and setting

$$\mathcal{M}': \mathcal{F}(\mathbf{x}) \rightarrow \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}}) \subset \overline{\mathbb{Q}\{\mathbf{X}\}}^\times, \\ x_i \mapsto e(X_i).$$

The map $X_i \mapsto e(X_i) - 1$ determines an algebra homomorphism $\overline{\mathbb{Q}\{\mathbf{X}\}} \rightarrow \overline{\mathbb{Q}\{\mathbf{X}\}}$ which sends $\mathcal{M}(w)$ to $\mathcal{M}'(w)$ for any $w \in F = \mathcal{F}(\mathbf{x})$. Therefore, if \mathcal{M}' is injective so is \mathcal{M} .

Let $N = \ker \mathcal{M}'$ and $L = F/N$. We shall prove that N coincides with the kernel of Higman's homomorphism $F \rightarrow (L, A)$ and this, by Lemmas 7 and 10, will imply that N is trivial. For this purpose, we shall embed (L, A) into a bigger loop, namely the loop of group-like elements of a Hopf-algebraic version of Higman's construction (L, A) .

5.2. Higman's construction for Hopf algebras. Let $m(\mathbf{X})$ be the set of all non-associative monomials on \mathbf{X} of degree ≥ 1 and T the set of symbols

$$\{t_1, \dots, t_n\} \sqcup \{t(m_1, m_2) \mid m_1, m_2 \in m(\mathbf{X})\}$$

with degrees

$$|t_1| = \dots = |t_n| = 1 \quad \text{and} \quad |t(m_1, m_2)| = |m_1| + |m_2|,$$

where $|X_1| = \dots = |X_n| = 1$. Write $\mathbb{Q}[T]$ for the usual commutative and associative algebra on T with the structure of a Hopf algebra obtained by declaring all elements of T to be primitive.

Define a linear map

$$t: \mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}\{\mathbf{X}\} \rightarrow \text{span}\langle T \rangle$$

by setting $t(m_1 \otimes m_2) = t(m_1, m_2)$, $t(m_1 \otimes 1) = t(1 \otimes m_2) = t(1 \otimes 1) = 0$ and let

$$t^*: \mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}\{\mathbf{X}\} \rightarrow \mathbb{Q}[T]$$

be the coalgebra morphism

$$t^*(\mu \otimes \mu') = \epsilon(\mu)\epsilon(\mu')1 + \sum_{k \geq 1} \frac{1}{k!} t(\mu_{(1)}, \mu'_{(1)}) \dots t(\mu_{(k)}, \mu'_{(k)}).$$

We shall use the same notation t and t^* for the extensions of these maps to maps between the respective completions of $\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}\{\mathbf{X}\}$, $\text{span}\langle T \rangle$ and $\mathbb{Q}[T]$ with respect to the degree.

The maps t and t^* are related in the following way: for any $g, g' \in \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}})$ we have

$$t^*(g \otimes g') = \sum_{k \geq 0} \frac{1}{k!} t(g \otimes g')^k = \exp(t(g \otimes g')) \in \overline{\mathbb{Q}[T]},$$

where \exp is the usual exponential series.

Lemma 12. *The elements $\exp(t_1), \dots, \exp(t_n)$ and $t^*(g \otimes g')$, where $g, g' \in \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}}) \setminus \{1\}$, freely generate a multiplicative abelian subgroup of $\mathcal{G}(\overline{\mathbb{Q}[T]})$.*

Proof. Assume that

$$\exp(t_1)^{e_1} \dots \exp(t_n)^{e_n} t^*(g_1 \otimes g'_1)^{d_1} \dots t^*(g_m \otimes g'_m)^{d_m} = 1$$

for some $g_1, g'_1, \dots, g_m, g'_m \in \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}}) \setminus \{1\}$ with $(g_i, g'_i) \neq (g_j, g'_j)$ if $i \neq j$, and some integers $e_1, \dots, e_n, d_1, \dots, d_m$. Then

$$\exp(e_1 t_1 + \dots + e_n t_n + d_1 t(g_1 \otimes g'_1) + \dots + d_m t(g_m \otimes g'_m)) = 1$$

and

$$e_1 t_1 + \dots + e_n t_n + d_1 t(g_1 \otimes g'_1) + \dots + d_m t(g_m \otimes g'_m) = 0.$$

Since $\{t_1, \dots, t_n\}$ and $\{t(m_1 \otimes m_2) \mid m_1, m_2 \in m(\mathbf{X})\}$ are algebraically independent, we have $e_1 = \dots = e_n = 0$ and

$$t(d_1 g_1 \otimes g'_1 + \dots + d_m g_m \otimes g'_m) = d_1 t(g_1 \otimes g'_1) + \dots + d_m t(g_m \otimes g'_m) = 0.$$

The kernel of $t: \overline{\mathbb{Q}\{\mathbf{X}\}} \otimes \overline{\mathbb{Q}\{\mathbf{X}\}} \rightarrow \overline{\text{span}\langle T \rangle}$ is

$$\overline{\mathbb{Q}\{\mathbf{X}\}} \otimes 1 + 1 \otimes \overline{\mathbb{Q}\{\mathbf{X}\}}$$

so that

$$d_1 \cdot g_1 \otimes g'_1 + \dots + d_m \cdot g_m \otimes g'_m = \mu \otimes 1 + 1 \otimes \eta$$

for some $\mu, \eta \in \overline{\mathbb{Q}\{\mathbf{X}\}}$. As $g_1, g'_1, \dots, g_m, g'_m \in \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}}) \setminus \{1\}$ and since different group-like elements are linearly independent [1, Theorem 2.1.2], we see that $d_1 = \dots = d_m = 0$. \square

Now, define a new product on $\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]$ by

$$(5.1) \quad (x \otimes \alpha)(y \otimes \beta) = \sum x_{(1)} y_{(1)} \otimes t^*(x_{(2)} \otimes y_{(2)}) \alpha \beta.$$

With this product, both $\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]$ and $\overline{\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]}$ are connected bialgebras. Consider the homomorphism

$$\begin{aligned} \widetilde{\mathcal{M}}': \mathcal{F}(\mathbf{x}) &\rightarrow \mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]}) \\ x_i &\mapsto e(X_i) \otimes \exp(t_i), \end{aligned}$$

where e is the same base for logarithms used for defining \mathcal{M}' . The formula

$$X_i \mapsto \log_e(e(X_i) \otimes \exp(t_i))$$

defines an injective algebra homomorphism

$$\phi: \overline{\mathbb{Q}\{\mathbf{X}\}} \rightarrow \overline{\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]}$$

and we have $\phi \circ \mathcal{M}' = \widetilde{\mathcal{M}}'$. In particular, for any words $w_1, w_2 \in \mathcal{F}(\mathbf{x})$ the equality

$$\mathcal{M}'(w_1) = \mathcal{M}'(w_2)$$

holds if and only if $\widetilde{\mathcal{M}}'(w_1) = \widetilde{\mathcal{M}}'(w_2)$.

Now, by definition, L is a subloop of $\mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\}})$ and Lemma 12 gives an natural injective homomorphism of (L, A) into $\mathcal{G}(\overline{\mathbb{Q}\{\mathbf{X}\} \otimes \mathbb{Q}[T]})$. Moreover, on L the map ϕ coincides with the map $L \rightarrow (L, A)$ and, therefore, as mentioned before, Lemmas 7 and 10 imply that \mathcal{M}' is injective.

5.3. **The commutative case.** The proof of the injectivity of \mathcal{M}_c involves minor changes:

- denote by $m_c(\mathbf{X})$ the set of all monomials of degree ≥ 1 in the commuting variables X_1, \dots, X_n ;
- define the set T as $\{t_1, \dots, t_n\} \sqcup \{t(m_1, m_2) \mid m_1, m_2 \in m_c(\mathbf{X})\}$ where we assume that $t(m_1, m_2) = t(m_2, m_1)$ for all $m_1, m_2 \in m_c(\mathbf{X})$;
- define the coalgebra morphism

$$t^*: \mathbb{Q}_c\{\mathbf{X}\} \otimes \mathbb{Q}_c\{\mathbf{X}\} \rightarrow \mathbb{Q}[T]$$

as before. The symmetry of t implies $t^*(\mu \otimes \mu') = t^*(\mu' \otimes \mu)$ for all $\mu, \mu' \in \mathbb{Q}_c\{\mathbf{X}\}$;

- write $\mathbb{Q}_c\{\mathbf{X}\} \otimes \mathbb{Q}[T]$ for the commutative bialgebra with the product given by (5.1);
- note that Lemma 12 trivially holds when $\overline{\mathbb{Q}\{\mathbf{X}\}}$ is replaced by $\overline{\mathbb{Q}_c\{\mathbf{X}\}}$;
- let $\mathcal{M}'_c: \mathcal{F}_c\{\mathbf{x}\} \rightarrow \mathcal{G}(\overline{\mathbb{Q}_c\{\mathbf{X}\}})$ and $\widetilde{\mathcal{M}}'_c: \mathcal{F}_c\{\mathbf{x}\} \rightarrow \mathcal{G}(\overline{\mathbb{Q}_c\{\mathbf{X}\} \otimes \mathbb{Q}[T]})$ be the homomorphisms determined by $\mathcal{M}'_c(x_i) = e(X_i)$ and $\widetilde{\mathcal{M}}'_c(x_i) = e(X_i) \otimes \exp(t_i)$ for some base for logarithms $e(X)$;
- fix a total order on $W(\mathbf{x})$ and call a word in $W(\mathbf{x})$ *reduced* if none of its components is the left-hand side of any of the equations

$$\begin{array}{lll} uv = vu \ (u < v) & u/v = v \setminus u & (v \setminus u) \setminus u = v \\ v \setminus (uv) = u & u \setminus (uv) = v & (u \setminus v)u = v \\ ev = v & u(u \setminus v) = v & e \setminus v = v \\ ue = u & & v \setminus v = e; \end{array}$$

- in the definition of the loop (L, A) , take the symbols $\langle l_1, l_2 \rangle$ to be symmetric in the sense that $\langle l_1, l_2 \rangle = \langle l_2, l_1 \rangle$.

With these new definitions Lemma 9 (that is, Higman's Lemma 6) remains true, and the injectivity of \mathcal{M}_c follows from it in the very same fashion as in the non-commutative case. For the sake of completeness, we include the proof of the commutative version of Lemma 9 here, although it follows Higman's original proof very closely.

5.4. **Proof of the commutative version of Lemma 9.** First, we observe that $w' \neq e$ since $w' \notin \text{Comp}(w)$.

The case when $w' = x_i$ is straightforward: $x_i = w' \notin \text{Comp}(w)$ implies that the coefficient of x_i in $\psi(w')$ is 1 while in $\psi(w)$ it is 0. Therefore, we only have to consider two cases: (1) $w' = uv$ and (2) $w' = u \setminus v$, where both u and v are reduced words. As w' is reduced, we have $u \neq e$. In fact, $\alpha(u) \neq 1$, the unit element of L , since $\alpha(u) = 1 = \alpha(e)$ implies, by hypothesis, that either $u = e$, a contradiction, or $\{u, e\} = \{w, w'\}$, which is not possible since $w' \neq u, e$.

In what follows, we will often consider two elements, say c_1 and c_2 , in $\text{Comp}(w') \cup \text{Comp}(w)$ with $\alpha(c_1) = \alpha(c_2)$. By hypothesis, this implies that either $c_1 = c_2$ or $\{w', w\} = \{c_1, c_2\}$. It will be clear that $w' \neq c_1, c_2$ (usually c_1 and c_2 will be either e , components of w or components of w' different from w') so we will conclude that $c_1 = c_2$ without further explanation.

5.4.1. *Case $w' = uv$.* First we observe that $\alpha(v) \neq 1$. Indeed, $\alpha(v) = 1 = \alpha(e)$ would imply that $v = e$ so that $w' = ue$ is not reduced, a contradiction. This ensures that $\langle \alpha(u), \alpha(v) \rangle$ is a generator of A . We will prove that the coefficient of $\langle \alpha(u), \alpha(v) \rangle$ in $\psi(\tau)$ is zero for any $\tau \in \{w, u, v\}$, which will allow us to conclude that the coefficient of $\langle \alpha(u), \alpha(v) \rangle$ in $\psi(w)$ is zero while in $\psi(w')$ it equals to one. To this end, assume that the coefficient of $\langle \alpha(u), \alpha(v) \rangle$ in $\psi(\tau)$ is non-zero and observe that $w' \notin \text{Comp}(\tau)$. There are two possibilities:

- (1) τ has a component $\tau_1\tau_2$ with $\{\alpha(\tau_1), \alpha(\tau_2)\} = \{\alpha(u), \alpha(v)\}$.
 - If $\alpha(\tau_1) = \alpha(u)$ and $\alpha(\tau_2) = \alpha(v)$ then $\tau_1 = u$ and $\tau_2 = v$. Thus $\tau = uv = w'$, a contradiction.
 - If $\alpha(\tau_1) = \alpha(v)$ and $\alpha(\tau_2) = u$ then $\tau_1 = v$, $\tau_2 = u$ and $\tau = vu$. Both τ and w' are reduced so $u \geq v$ and $v \geq u$. Hence $u = v$ and $\tau = uu = w'$, a contradiction.
- (2) τ has a component $\tau_1 \setminus \tau_2$ with $\{\alpha(\tau_1), \alpha(\tau_1 \setminus \tau_2)\} = \{\alpha(u), \alpha(v)\}$.
 - If $\alpha(\tau_1) = \alpha(u)$ and $\alpha(\tau_1 \setminus \tau_2) = \alpha(v)$ then $\tau_1 = u$ and
 - either $\tau_1 \setminus \tau_2 = v$, which implies that $w' = uv = \tau_1(\tau_1 \setminus \tau_2)$ is not reduced, a contradiction,
 - or $w' = \tau_1 \setminus \tau_2$ and $w = v$, which is again a contradiction since $w' \notin \text{Comp}(\tau)$.
 - If $\alpha(\tau_1) = \alpha(v)$ and $\alpha(\tau_1 \setminus \tau_2) = \alpha(u)$ then $\tau_1 = v$ and $\tau_1 \setminus \tau_2 = u$. Thus $w' = (\tau_1 \setminus \tau_2)\tau_1$ is not reduced, a contradiction.

5.4.2. *Case $w' = u \setminus v$.* We first observe that $\alpha(u \setminus v) \neq 1$. Indeed, $\alpha(u \setminus v) = 1$ would imply $\alpha(u) = \alpha(v)$ so that $u = v$ and $w' = u \setminus u$ is not reduced, a contradiction. This ensures that $\langle \alpha(u), \alpha(u \setminus v) \rangle$ is a generator of A . We will prove that the coefficient of $\langle \alpha(u), \alpha(u \setminus v) \rangle$ in $\psi(\tau)$ is zero for any $\tau \in \{w, u, v\}$, which will allow us to conclude that the coefficient of $\langle \alpha(u), \alpha(u \setminus v) \rangle$ in $\psi(w)$ is zero while it is -1 in $\psi(w')$. To this end, assume that the coefficient of $\langle \alpha(u), \alpha(u \setminus v) \rangle$ in $\psi(\tau)$ is non-zero and observe that $w' \notin \text{Comp}(\tau)$. There are two possibilities:

- (1) τ has a component $\tau_1\tau_2$ with $\{\alpha(\tau_1), \alpha(\tau_2)\} = \{\alpha(u), \alpha(u \setminus v)\}$.
 - If $\alpha(\tau_1) = \alpha(u)$ and $\alpha(\tau_2) = \alpha(u \setminus v)$ then $\tau_1 = u$ and $\alpha(v) = \alpha(u)\alpha(w') = \alpha(u)\alpha(\tau_2) = \alpha(\tau_1\tau_2)$. Thus
 - either $v = \tau_1\tau_2$, which implies $w' = \tau_1 \setminus (\tau_1\tau_2)$, a contradiction,
 - or $w' = \tau_1\tau_2$ and $w = v$, which is not possible since $w' \notin \text{Comp}(\tau)$.
 - If $\alpha(\tau_1) = \alpha(u \setminus v)$ and $\alpha(\tau_2) = \alpha(u)$ then $\tau_2 = u$ and $\alpha(\tau_1\tau_2) = \alpha(\tau_1)\alpha(\tau_2) = \alpha(\tau_2)\alpha(\tau_1) = \alpha(u)\alpha(u \setminus v) = \alpha(v)$. Thus, $\tau_1\tau_2 = v$ and $w' = u \setminus v = \tau_2 \setminus (\tau_1\tau_2)$ is not reduced, a contradiction.
- (2) τ has a component $\tau_1 \setminus \tau_2$ with $\{\alpha(\tau_1), \alpha(\tau_1 \setminus \tau_2)\} = \{\alpha(u), \alpha(u \setminus v)\}$.
 - If $\alpha(\tau_1) = \alpha(u)$ and $\alpha(\tau_1 \setminus \tau_2) = \alpha(u \setminus v)$ then $\tau_1 = u$ and $\alpha(v) = \alpha(u)\alpha(u \setminus v) = \alpha(\tau_1)\alpha(\tau_1 \setminus \tau_2) = \alpha(\tau_2)$ so $\tau_2 = v$. Hence $w' = u \setminus v = \tau_1 \setminus \tau_2 \in \text{Comp}(\tau)$, a contradiction.
 - If $\alpha(\tau_1) = \alpha(u \setminus v)$ and $\alpha(\tau_1 \setminus \tau_2) = \alpha(u)$ then $u = \tau_1 \setminus \tau_2$ and $\alpha(v) = \alpha(u)\alpha(u \setminus v) = \alpha(u \setminus v)\alpha(u) = \alpha(\tau_1)\alpha(\tau_1 \setminus \tau_2) = \alpha(\tau_2)$. Thus, $\tau_2 = v$ and $w' = u \setminus v = (\tau_1 \setminus \tau_2) \setminus \tau_2$ is not reduced, a contradiction.

REFERENCES

- [1] E. Abe, Hopf algebras. Cambridge University Press, Cambridge-New York (1980).
- [2] R.H. Bruck, A survey of binary systems. Springer Verlag, Berlin-Göttingen-Heidelberg (1958).

- [3] T. Evans, On multiplicative systems defined by generators and relations. I. Normal form theorems, Proc. Cambridge Phil. Soc. **47**, (1951), 637–49.
- [4] M. Hartl and B. Loiseau, On actions and strict actions in homological categories, Theory and Applications of Categories, **27**, no. 15, (2013), 347–392.
- [5] G. Higman, The lower central series of a free loop, Q. J. Math., **14**, no. 1, (1963), 131–140.
- [6] W. Magnus, A. Karrass, D. Solitar, Donald, Combinatorial group theory: Presentations of groups in terms of generators and relations. Interscience Publishers [John Wiley & Sons, Inc.], New York-London-Sydney (1966) Heldermann Verlag, Berlin, 1990.
- [7] J. Mostovoy, The Notion of Lower Central Series for Loops. In Sabinin, L., Sbitneva, L., Shestakov, I. (eds.) Non-associative algebra and its applications. pp. 291–298. Chapman & Hall/CRC-Press, Boca Raton, FL (2006)
- [8] J. Mostovoy, Nilpotency and Dimension Filtration for Loops. Commun. Algebra **36**, (2008), 1565–1579.
- [9] J. Mostovoy, J.M. Pérez Izquierdo, Dimension Filtration on Loops. Isr. J. Math. **158**, (2007), 105–118.
- [10] J. Mostovoy, J.M. Pérez Izquierdo, I. Shestakov, Nilpotent Sabinin algebras, J. Algebra, **419**, (2014), 95–123.
- [11] J. Mostovoy, J.M. Pérez Izquierdo, I. Shestakov, Hopf algebras in non-associative Lie theory, Bull. Math. Sci. **4**, no. 1, (2014), 129–174.
- [12] J. Mostovoy, J.M. Pérez Izquierdo, I. Shestakov, A Non-associative Baker-Campbell-Hausdorff formula, [arXiv:1605.00953](https://arxiv.org/abs/1605.00953) [math.RA].
- [13] J.M. Pérez Izquierdo, Algebras, hyperalgebras, nonassociative bialgebras and loops, Adv. Math. **208**, 834–876 (2007)
- [14] C.R.B. Wright, On the multiplication group of a loop, Illinois J. Math. **13**, no. 4, (1969), 660–673.

DEPARTAMENTO DE MATEMÁTICAS, CINVESTAV-IPN, COL. SAN PEDRO ZACATENCO, CIUDAD DE MÉXICO, C.P. 07360, MEXICO

E-mail address: jacob@math.cinvestav.mx

DEPARTAMENTO DE MATEMÁTICAS Y COMPUTACIÓN, UNIVERSIDAD DE LA RIOJA, EDIFICIO CCT - C/ MADRE DE DIOS, 53, 26006, LOGROÑO, LA RIOJA, SPAIN

E-mail address: jm.perez@unirioja.es

INSTITUTO DE MATEMATICA E ESTATSTICA, UNIVERSIDADE DE SÃO PAULO, CAIXA POSTAL 66281, SÃO PAULO, SP 05311-970, BRAZIL

E-mail address: shestak@ime.usp.br